

Ancilla-Driven Universal Quantum Computation

Janet Anders,¹ Daniel K. L. Oi,² Elham Kashefi,³ Dan E. Browne,¹ and Erika Andersson⁴

¹*Department of Physics & Astronomy, University College London, London WC1E 6BT, UK*

²*SUPA, Department of Physics, University of Strathclyde, Glasgow G4 0NG, UK*

³*School of Informatics, University of Edinburgh, Edinburgh, EH8 9AB, UK*

⁴*SUPA, Department of Physics, Heriot-Watt University, Edinburgh EH14 4AS, UK*

We propose a method of manipulating a quantum register remotely with the help of a single ancilla that “steers” the evolution of the register. The fully controlled ancilla qubit is coupled to the computational register solely via a *fixed* unitary two-qubit interaction, E , and then measured in suitable bases. We characterize all interactions E that induce a unitary, step-wise deterministic measurement back-action on the register sufficient to implement any arbitrary quantum channel. Our scheme offers significant experimental advantages for implementing computations, preparing states and performing generalized measurements as no direct control of the register is required.

PACS numbers: 03.67.-a,03.67.Lx

Introduction. – The two best-known strategies of performing a quantum computation are the gate-based and measurement-based model (MBQC). In the former, a computation is performed by actively manipulating individual register qubits by a network of logical gates. The required control of the register is very challenging to realize in experiments. MBQC is an alternative strategy that relies on the powerful effect of measurements on entangled quantum systems [1, 2]. A computation is here implemented “passively”, as a sequence of adaptive single-qubit measurements on an entangled multi-partite resource state and realized in experiments [3] were single qubit measurements are “cheap”. Hard work, however, goes into the construction of the initial resource state.

In this paper we introduce a hybrid model that is tailored to fit many experimental settings. The scheme utilizes a single fully controlled ancilla qubit, which is coupled sequentially to one or, at most, two qubits of a register via a *fixed* entangling operation, E , to enable universal state preparation [4]. After each coupling the ancilla is measured in a suitable basis, providing a back-action onto the register which implements unitary evolution of the register. Moreover, using an additional, second ancilla qubit any Positive Operator Valued Measurement (POVM), and thus any quantum channel, can be realized. The computation requires no direct control of the register nor the preparation of a large entangled state. The processing of information is driven by active manipulation of the ancilla alone and we shall call the model *Ancilla-Driven Quantum Computation* (ADQC).

Previous attempts to construct ‘remotely controlled’, deterministic and universal quantum state preparators have concluded this to be impossible [5, 6]. These schemes use, like ours, additional ‘programmable qubits’, i.e. ancillas, that are coupled to the register with a fixed interaction. Our results highlight that the existing no-go theorems do not apply when *feedback* within the programmable part is allowed and a final *local* redefinition of the computational basis of the register is performed.

The key advantage of ADQC is that register qubits are only addressed with a single coupling operation, E . No further operation, neither unitary nor measurement, is required. This provides architectural advantages for many experimental situations as the computational register can be separated from state preparation and measurement, and does not require bespoke control. This lends itself to systems where long-lived but static qubits are addressed by more mobile ancilla qubits subject to a single entangling interaction. There are many physical systems which possess the required features and interactions, such as neutral atoms in optical lattices [7], micro ion trap arrays [8], nuclear-electron spin systems [9] and cavity QED-superconducting qubits [10]. ADQC is also advantageous in physical systems where measurements are destructive, i.e. experiments with photons, as the measurement never acts on the register and leaves it intact for further manipulation.

Example: Control-Z & Hadamard interaction. – The idea behind ADQC is simple yet surprisingly powerful, see Fig. 1. The ancilla, A , is sequentially prepared, then entangled with a fixed interaction E_{AR} to a register

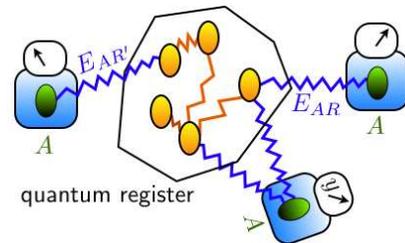


FIG. 1: Illustration of an ancilla-driven computation on a register consisting of several qubits. A single ancilla, A , is sequentially coupled to one, or at most two, register qubits, R and R' etc., and measured. The coupling, E_{AR} , is fixed throughout the computation while the measurements on the ancilla, indicated by the arrows, can differ.

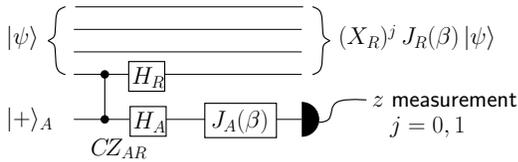


FIG. 2: Ancilla-driven implementation of a single qubit rotation, $J_R(\beta)$, on a register qubit R . The initial state of the total register can be a pure state, $|\psi\rangle$, or accordingly for a mixed state. The ancilla and register qubits are first coupled with $E_{AR} = H_A H_R CZ_{AR}$. The rotation $J(\beta)$ is then implemented on the fully controlled ancilla and transferred to the register qubit by measuring the ancilla in the z -basis. The result of the measurement, $j = 0, 1$, determines if an X correction appears on the register qubit.

qubit, R , and then measured. The induced back-action onto the register is what “steers” the register to the desired state [11]. An example of a universal interaction between register and ancilla is the Control-Z interaction followed by local Hadamards, $H = (X + Z)/\sqrt{2}$ with X, Y, Z the Pauli matrices,

$$E_{AR} = H_A H_R CZ_{AR}, \quad (1)$$

where Control-Z is given by $CZ = \mathbb{1} - 2|11\rangle\langle 11|$. This is reminiscent of MBQC where resource states for computation are constructed using the CZ operation [1, 2].

Any arbitrary single qubit unitary can be decomposed into four rotations, $J(\beta) = H e^{i\frac{\beta}{2}X}$, as $U = e^{i\alpha} J(0) J(\beta) J(\gamma) J(\delta)$ with parameters β, γ, δ (Euler angles) and α (global phase) in \mathbb{R} [12]. To implement a rotation $J_R(\beta)$ on the register in the ancilla-driven model the ancilla is first prepared in the state $|+\rangle_A$ and then coupled to the qubit R via E_{AR} , see Fig. 2. Instead of acting on the register qubit the rotation $J_A(\beta)$ is applied to the ancilla and transferred to the register qubit by measuring the ancilla in the computational z -basis $|j\rangle$ with $j = 0, 1$. Alternatively, the ancilla can be measured immediately in the rotated basis $|\beta_+\rangle_A = \cos\frac{\beta}{2}|0\rangle_A + i\sin\frac{\beta}{2}|1\rangle_A$ and $|\beta_-\rangle_A = \cos\frac{\beta}{2}|1\rangle_A + i\sin\frac{\beta}{2}|0\rangle_A$. The implemented operation on the register qubit is

$$A\langle j|J_A(\beta)E_{AR}|+\rangle_A = U_R(j)J_R(\beta), \quad (2)$$

with (fixed) Pauli correction $U_R(j) = (X_R)^j$ that depends on the measurement outcome j of the ancilla. (We neglect global phases of states and unitaries as they are physically insignificant.) The correction can be removed by changing the ancilla measurement bases of future computational operations, cf. [1, 2] and [13].

Arbitrary single qubit unitaries composed with an entangling operation, such as the CZ gate, form a universal set of gates, allowing the construction of any unitary evolution. To entangle two register qubits, R and R' , they each interact with the ancilla via the same operation E ,

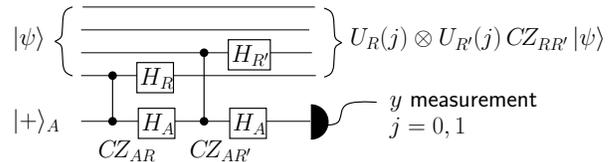


FIG. 3: Ancilla-driven implementation of a Control-Z gate, $CZ_{RR'}$, on two register qubits R and R' . Both register qubits are coupled with $E_{AR(A R')} = H_A H_{R(R')} CZ_{AR(A R')}$ to the ancilla which is then measured in the y -basis. The corrections $U_R(j)$ and $U_{R'}(j)$ are local and can be applied through ancilla-driven single qubit rotations.

see Fig. 3. A y -measurement of the ancilla then mediates the entangling operation between the register qubits,

$$A\langle y_j|E_{AR}E_{AR'}|+\rangle_A = U_R(j) \otimes U_{R'}(j) CZ_{RR'}. \quad (3)$$

This is a Control-Z operation up to local corrections $U_{R,R'}(j) = H_{R,R'} \left(\frac{\mathbb{1}_{R,R'} + iZ_{R,R'}}{\sqrt{2}} \right) (Z_{R,R'})^j$ that again depend on the outcome j of the ancilla measurement. $U_R(j)$ and $U_{R'}(j)$ can be applied explicitly as single qubit operations as described above. Thus ADQC with the interaction being fixed to $E_{AR} = H_A H_R CZ_{AR}$ allows the implementation of any unitary evolution, or *universal state preparation*, of the register [14].

General interactions for ADQC.— A fundamental question in the context of new models for quantum computation is to specify *all* entangling operations, E , that lead to universality [4, 15]. To add structure to this question one can restrict to computations with a number of desirable properties. An important requirement for the working of ADQC is that no operation, including any corrections, ever needs direct implementation on the register. We therefore consider unitary, step-wise deterministic, “tensor-commuting” (as defined below) computations; i.e. by adapting ancilla measurement bases alone corrections on the register can be absorbed and the computation remains deterministic at every step [16, 17].

While in MBQC with the cluster state only standard X, Y and Z corrections occur, here we allow a broader class which we entitle *generalized Pauli corrections*. This is the class of all single-qubit Hermitian unitaries P which satisfy $\text{tr}[P] = 0$. These can be parametrized as $P(a, b, c) = aX + bY + cZ$ with $a, b, c \in \mathbb{R}$ and $a^2 + b^2 + c^2 = 1$. Let us now introduce the canonical decomposition [18, 19] for two-qubit unitaries, $E_{AR} = (W'_A \otimes W_R) D_{AR} (V'_A \otimes V_R)$, which separates the essential non-local part

$$D_{AR}(\alpha_x, \alpha_y, \alpha_z) = e^{-i(\alpha_x X_A \otimes X_R + \alpha_y Y_A \otimes Y_R + \alpha_z Z_A \otimes Z_R)} \quad (4)$$

with $0 \leq \alpha_{x,y,z} \leq \pi/4$ from local single qubit unitaries on the register, V_R, W_R , and the ancilla, V'_A, W'_A . To allow composition of operations to arbitrarily large computations all corrections on register qubits need to interchange with future entangling operations, D_{AR} , in

such a way that they remain localized, i.e. the resulting correction is a tensor product between the register and ancilla. This allows the corrections on each register qubit to shift through the computational pattern and accumulate at the final step where they can be removed by a *local* redefinition of the computational basis [20]. If there exist such corrections, we say that the entangling operation, D_{AR} , *tensor-commutes* with the corrections [21], i.e. $D_{AR} P_R(a, b, c) D_{AR}^\dagger = P_A(\tilde{a}, \tilde{b}, \tilde{c}) \otimes P_R(a', b', c')$ where \tilde{P}_A and P'_R are also generalized Pauli transformations (or the identity, see [22]).

The key result of this paper is that only two classes of couplings have the potential to be universal as summarized in the theorem below.

Theorem. *The interactions, E_{AR} , between any register qubit, R , and the ancilla, A , that result in a i) unitary, step-wise deterministic evolution of the register, that ii) tensor-commute with corrections and that iii) admit universal state preparation of the register using ADQC, are locally equivalent to (i.e. D_{AR} is of the form) the Ising model or the Heisenberg XX model with maximal coupling strength $\alpha = \pi/4$ or $\alpha_x = \alpha_y = \pi/4$.*

Moreover, any generalized measurement, or POVM, on the register can be performed in the ancilla-driven model with the (repeated) help of a second ancilla that introduces extra degrees of freedom to form a suitable Neumark extension of the register's state [23, 24]. This is of interest especially when measurements on the register would remove the physical qubit, such as photon measurements. In ADQC, the destructive measurement is instead made on the ancilla and the register qubits remain for future operations.

The importance of the theorem is in the *only if* part which proves for the first time the necessity of this type of building block. The two classes of interactions are equivalent to the Control-Z gate, as shown constructively in the example above, and the Control-Z+SWAP gate, where $CZ+SWAP = |00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| - |11\rangle\langle 11|$. Both interactions are maximally entangling [19, 25] and Clifford operations [26].

The proof of the theorem is involved and technical details can be found in [22]. An outline of the arguments is given here. When the ancilla with initial state $|+\rangle_A$ and a single register qubit are coupled, and the ancilla is subsequently measured in $|\pm\rangle_A$ then the state $|\psi\rangle$ of the register (and similarly for mixed states) becomes

$$|\psi\rangle \mapsto \frac{K_R^\pm}{\sqrt{p^\pm}} |\psi\rangle, \quad (5)$$

where the Kraus operators K_R^\pm are given by

$$K_R^\pm = {}_A\langle \pm | E_{AR} | + \rangle_A = {}_A\langle \pm_{\theta, \phi} | W_R D_{AR} V_R | +_{\gamma, \delta} \rangle_A, \quad (6)$$

and $p^\pm = \text{tr}[K_R^{\pm\dagger} K_R^\pm]$ are the probabilities of obtaining measurement outcome $+$ or $-$. Here we substituted $| +_{\gamma, \delta} \rangle_A = \cos \frac{\gamma}{2} | 0 \rangle_A + e^{i\delta} \sin \frac{\gamma}{2} | 1 \rangle_A = V'_A | + \rangle_A$ and

$|\pm_{\theta, \phi}\rangle_A = W_A^\dagger |\pm\rangle_A$ where γ, δ, θ and ϕ denote ancilla parameters contained in V'_A and W'_A .

In a step-wise deterministic computation the Kraus operators must necessarily be proportional to unitaries and this implies that one of the α 's, say α_z , must vanish. Additionally, the two Kraus operations shall relate to another via a generalized Pauli, $K_R^-/\sqrt{p^-} = e^{i\Delta} P_R K_R^+/\sqrt{p^+}$, where Δ is an unimportant global phase. Moreover, the non-local part of the interaction, D_{AR} , must tensor-commute with this correction P_R . These requirements restrict the interaction to four classes, $D_{AR}(\pi/4, \pi/4, 0)$, $D_{AR}(0 < \alpha_x < \pi/4, \pi/4, 0)$, $D_{AR}(\pi/4, 0, 0)$ and $D_{AR}(0 < \alpha < \pi/4, 0, 0)$, each with their individual sets of acceptable ancilla parameters $\gamma, \theta, \delta, \phi$ and sets $P(a, b, c)$ with a, b, c of tensor-commuting corrections.

However, two of these classes are not sufficient for universal state preparation. Ising interactions with non-maximal interaction strength, $D_{AR}(0 < \alpha < \pi/4, 0, 0)$, can be used to steer unitary, step-wise deterministic evolutions of a register qubit. Yet the ancilla parameters are so restricted that the set of implementable single qubit unitaries lies in a plane of the Bloch sphere and $D_{AR}(0 < \alpha < \pi/4, 0, 0)$ (plus local unitaries) is *not universal*. For Heisenberg models with non-maximal coupling strength, $D_{AR}(0 < \alpha_x < \pi/4, \pi/4, 0)$, it is impossible to *compose* several single qubit operations after another while preserving step-wise determinism, see [22] for details. This leaves only two universal classes, $D_{AR}(\pi/4, 0, 0)$ and $D_{AR}(\pi/4, \pi/4, 0)$, which are locally equivalent to CZ_{AR} and $CZ_{AR} + \text{SWAP}_{AR}$. This leads to the theorem.

We note that the choice of appropriate *local unitaries* in E_{AR} is not trivial - CZ alone can not steer all register evolution as no basis change can be achieved at the register qubit. However, we showed in the example above that together with local Hadamards that enable a basis change, the CZ interaction can be made universal. For the $CZ+SWAP$ interaction it is easy to verify that the ADQC model is identical to the one-way model [1] and hence allows universal state preparation, as the role of ancilla and register qubits are simply swapped.

Physical systems suitable for ADQC. - ADQC is suited to many physical realizations, e.g. a register of atoms trapped in an optical lattice addressed by ancilla marker atoms [27], which interact via cold collisions to generate control-Z gates [7]; similarly an array of ions in microtraps and an ancilla read-write ion that interacts by laser-induced state-dependent pushing forces [8]. Using optimized control pulses [28] it may be possible to generate the E_{AR} operation efficiently and robustly in a single step. We can also consider different systems for the role of register and ancilla, e.g. a cavity QED [29] register, and Rydberg atoms traversing them as ancillas [30]. While 'static' qubit field states are hard to manipulate directly,

‘flying’ Rydberg atoms are easily controlled by lasers and measured by field-ionization. We note that [30] suggests entangling two cavity qubits by the sequential interaction of the XX -type with an ancilla Rydberg atom which is then measured (c.f. Eq.(3)). However different cavity qubit rotations are achieved by varying the control pulse between the register and ancilla, while ADQC requires only a single register-ancilla operation.

Another hetero-qubit scheme uses nuclear and electron spins, e.g. an array of long-lived phosphorus donor nuclear spins in silicon as the register [9], and electron ancillas move around the array by charge transport by adiabatic passage (CTAP) [31]. Control and characterization of the nuclear-electron interaction is reduced to optimization of a single two-qubit unitary, simplifying the task considerably, especially for qubits subject to manufacturing variation and tolerances [32]. We can exploit spin-orbit effects to introduce anisotropies into the Heisenberg interaction [33, 34] which allow Ising-type entangling unitaries to be generated [35]. Finally, superconducting qubits coupled with an effective Hamiltonian of the $XX + YY$ type via a superconducting microwave stripline [10] are also good candidates for ADQC.

In summary, ADQC is a practical method of implementing any quantum channel on a quantum register *without direct manipulation*, when an entangling operation E_{AR} is naturally available. Imperfections in the interaction could arise in a number of ways, for example in decoherence and in the timing and finite duration of the measurements. An important project for future work is to investigate how quantum error correction techniques can be employed to deliver fault tolerance in the ADQC model and allow implementation in a yet broader class of physical systems.

The equivalence to other computational schemes makes ADQC a valuable model that shifts the question of universal resources away from resource states and their structure, and focuses instead on basic building blocks. These can be characterized systematically by requiring properties sufficient for universal computation and showing why some fail. In the future this approach can be adapted to investigate computations with relaxed properties. For instance, one might not require the computation to be step-wise deterministic, similar to the computation using computational tensor network states [15]. We expect that these correspond to unitary Kraus operators, i.e. one of the α ’s must vanish, however the branching relation could be non-Pauli but instead any finite root of $\mathbb{1}$. This would lead to schemes based on Ising or Heisenberg interactions with smaller coupling strength, $\alpha < \pi/4$.

We thank Mark Hillary for insightful discussions. JA is funded by the EPSRC’s QIPIRC network in the UK. DEB thanks the National Science Foundation of Singapore. JA and DEB acknowledge QNET support in the UK. We all thank the Scottish Universities Physics Alliance and QUISCO.

- [2] H. J. Briegel, *et al.*, Nature Physics **5** 19 (2009); D.E. Browne, H.J. Briegel, Chapter 5.3 in *Lecture Notes on Quantum Information*, Wiley (2006), arXiv:quant-ph/0603226.
- [3] P. Walther, *et al.*, Nature **434**, 169 (2005).
- [4] M. Van der Nest, *et al.*, Phys. Rev. Lett. **97**, 150504 (2006).
- [5] M.A. Nielsen, I.L. Chuang, Phys. Rev. Lett. **79**, 321 (1997).
- [6] S.F. Huelga, *et al.*, Phys. Rev. A **63**, 042303 (2001); S.F. Huelga, *et al.*, Phys. Rev. A **65**, 042316 (2002).
- [7] D. Jaksch, *et al.*, Phys. Rev. Lett. **82**, 1975 (1999).
- [8] J. I. Cirac, P. Zoller, Nature **404**, 579 (2000).
- [9] B. E. Kane, Nature **393**, 133 (1998).
- [10] J. Majer, *et al.*, Nature **449**, 443 (2007).
- [11] H.M. Wiseman, *et al.*, Phys. Rev. Lett. **98**, 140402 (2007).
- [12] V. Danos, E. Kashefi, P. Panangaden, Phys. Rev. A **72**, 064301 (2005).
- [13] E. Kashefi, *et al.*, Elec. Not. Theo. Comp. Sci. **249**, 307 (2009).
- [14] The computational patterns for ADQC generated with the *non-commuting* operators, $E_{AR} = H_A H_R CZ_{AR}$, and MBQC can be translated to one another by use of a novel type of open graph states, the twisted graph states [13]. This allows to optimize coupling sequences for ADQC and find patterns with the smallest depth.
- [15] D. Gross, J. Eisert, Phys. Rev. Lett. **98**, 220503 (2007).
- [16] V. Danos, E. Kashefi, Phys. Rev. A **74**, 052310 (2006).
- [17] D.E. Browne, *et al.*, New J. Phys. **9**, 250 (2007).
- [18] J. Zhang, *et al.*, Phys. Rev. A **67**, 042313 (2003).
- [19] B. Kraus, J.I. Cirac, Phys. Rev. A **63**, 062309 (2001).
- [20] The final correction can also be implemented explicitly in the ancilla-driven manner. This would be the only non-deterministic instance where repeated application may be necessary.
- [21] These requirements also permit a standardization procedure as defined for the MBQC model [36].
- [22] E. Kashefi, *et al.*, submitted to Th. Comp. Sci. 2009.
- [23] E. Andersson, D.K.L. Oi, Phys. Rev. A **77**, 052104 (2008).
- [24] B. Reznik, Int. J. Quant. Inf. **4**(1), 181 (2006).
- [25] M. S. Leifer, *et al.*, Phys. Rev. A **67**, 012306 (2003).
- [26] D. Gottesman, PhD thesis, CalTech, Pasadena, (1997); S. Aaronson, D. Gottesman, Phys. Rev. A **70**, 052328 (2004).
- [27] T. Calarco *et al.*, Phys. Rev. A **70**, 012306 (2004).
- [28] U. V. Poulsen, *et al.*, arXiv:0910.4495 (2009); R. Nigmatullin, S. G. Schirmer, New J. Phys. **11**, 105032 (2009).
- [29] M. Brune, *et al.*, Phys. Rev. Lett. **101**, 240402 (2008).
- [30] V. Giovannetti, *et al.*, Phys. Rev. A **62**, 032306 (2000).
- [31] A.D. Greentree, *et al.*, Phys. Rev. B **70**, 235317 (2004).
- [32] S.G. Schirmer, D.K.L. Oi, Phys. Rev. A **80**, 022333 (2009).
- [33] K. V. Kavokin, Phys. Rev. B **64**, 075305 (2001).
- [34] L-A. Wu, D.A. Lidar, Phys. Rev. A **66**, 062314 (2002).
- [35] M. Borhani, D. Loss, Phys. Rev. A **71**, 034308 (2005).
- [36] V. Danos, E. Kashefi, P. Panangaden, Journal of the ACM **54** (2), 8 (2007).

[1] R. Raussendorf, H.J. Briegel, Phys. Rev. Lett. **86**, 910 (2001).